AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

Southern District of Ohio

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

LG Z832: FCCID: SRQ-Z831, IMEI: 869627024081713, S/N: 328C66800E39, SKU: DZTK4021

Case No. 3:20mj012
SHARON L. OVINGTON

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

SEE ATTACHMENT A

located in the _____ District of _____, there is now concealed *(identify the person or describe the property to be seized)*:

SEE ATTACHMENT B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
21 USC 846, 841(a)(1)	Conspiracy to possess with the intent to distribute and to distribute a controlled substance.

The application is based on these facts:

SEE ATTACHED AFFIDAVIT

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

SA Joseph Rossiter, USPIS
Printed name and title

Sworn to before me and signed in my presence.

Date: 01/03/2020

Judge's signature

City and state: Dayton, Ohio

Sharon L. Ovington, U.S. Magistrate Judge
Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF NEW YORK

IN THE MATTER OF THE SEARCH OF **LG-M153: IMEI: 354064064089453326, S/N: 709CQJZ945332, FCC ID: ZNFM150; ZTE Grand X Max2: SKU: DZTK4120, IMEI: 868962022957502, S/N: 320173713308; LG Z832: FCCID: SRQ-Z831, IMEI: 869627024081713, S/N: 328C66800E39, SKU: DZTK4021; Kyocera E4277: FCC ID: V65E4255, DEC: 268435459912517369, HEX: A0000027BEFFF9.** CURRENTLY LOCATED AT THE UNITED STATES POSTAL INSPECTION SERVICE, 1111 E 5TH ST, DAYTON, OH 45401.	Case No. 3:20 mj 012

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, **Joseph Rossiter,** being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—an electronic device—which is currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a United States Postal Inspector, having been so employed since May 2016. I am presently assigned to the Cincinnati Field Office, Pittsburgh Division of the Postal Inspection Service with investigative responsibility for southeast Indiana, and southern Ohio. Your Affiant completed United States Postal Inspection Service Basic Training in May 2016. This training involved narcotic investigation techniques, chemical field tests and training in the detection and identification of controlled substances being transported in the United States Mail. In addition to this formal training, I have worked since May 2016 with various federal, state and local law enforcement agencies on the investigation of the transportation of illegal drugs and their identification.

3. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

IDENTIFICATION OF THE DEVICE TO BE EXAMINED

4. The property to be searched is a black, LG-M153: IMEI: 354064064089453326, S/N: 709CQJZ945332, FCC ID: ZNFM150 (hereinafter referred to as "Device #1"), a black, ZTE Grand X Max2: SKU: DZTK4120, IMEI: 868962022957502, S/N: 320173713308 (hereinafter referred to as "Device #2"), a black LG Z832: FCCID: SRQ-Z831, IMEI: 869627024081713, S/N: 328C66800E39, SKU: DZTK4021 (hereinafter referred to as "Device #3") and Kyocera E4277: FCC ID: V65E4255, DEC: 268435459912517369, HEX: A0000027BEFFF9 (hereinafter referred to as "Device #4"). The Devices are currently located at the United States Postal Inspection Service Office, 1111 East 5th St, Dayton, OH 45401.

5. The applied-for warrant would authorize the forensic examination of the Device for the purpose of identifying electronically stored data particularly described in Attachment B.

PROBABLE CAUSE

6. On or about August 9, 2019, I intercepted a package (hereinafter, the "Package") at the Paul Laurence Dunbar Post Office in Dayton, OH. The Package is a Priority Mail box, bearing tracking number 9505 5144 6183 9219 5745 67, weighing approximately 15 ounces, postmarked August 7, 2019, addressed to "Staten Family 1310 DANNer Ave. DAyTON OH. 45417" with a return address of "MARKus Lewis 4326 LAurel CANyON #1 Studio City, CA. 91604."

7. On or about August 9, 2019, I obtained a federal search warrant which I then executed on the Package. Upon opening the Package, I removed a Priority Mail Flat Rate Envelope, which contained a Priority Mail Tyvek bag. Inside the Tyvek bag was a vacuumed sealed bag wrapped in paper towels. Inside the vacuumed sealed bag was approximately 280 grams of blueish circular pills, stamped consistent with oxycodone markings. A sample of the pills was thereafter sent to the Miami Valley Regional Crime Lab for forensic testing. Initial testing found the pills to be fentanyl, a schedule II controlled substance. The pills were not oxycodone.

8. On or about August 13, a controlled delivery was coordinated with other law enforcement agencies. A light sensor and GPS tracking device were placed inside the Package by law enforcement, prior to delivery. The Package was filled with 20 grams of the seized fentanyl pills, and a sham (made to appear like narcotics but is fake) substance vacuumed sealed in bag, to bring the Package back to its original weight. A United States Postal Inspector acting in an undercover capacity, then attempted to deliver the Package to 1310 Danner Ave, Dayton, OH 45417. Upon arriving at said address, the Postal Inspector knocked on the door and a black male suspect, later identified as Johnny MEDLAR, answered the door. The Postal Inspector asked if he was expecting a package for Staten, MEDLAR replied "yeah", and accepted and took the Package into the residence.

9. MEDLAR stayed inside the residence for a short period of time then exited with another black male later identified as Deshan FISHER, and got into a silver Chrysler 300. MEDLAR then drove the Chrysler 300 from the scene. The GPS tracker indicated that MELDAR still had the Package in his possession. The two suspects then drove to a residence located at 909 Maplehurst Ave, Dayton, OH 45402. Once there MEDLAR exited the vehicle and entered the residence. FISHER remained in the vehicle. These events were also witnessed by law enforcement acting in an undercover capacity.

10. Once inside 909 Maplehurst Ave, Dayton, OH 45402, law enforcement received a signal from a light indication sensor which indicated that the package was being opened. Law Enforcement moved in, and took MEDLAR into custody on the front porch of the residence. FISHER was removed from the vehicle and also taken in to custody. In MEDLAR's possession was the GPS and Light sensor device, together with the 20 grams of pills and the sham which he had placed down his pants after opening the Package. MEDLAR was subsequently released from police custody.

11. Devices #1, #2, #3 and #4 were seized from 1310 Danner Avenue, Dayton, OH 45417 during execution of the search warrant and have been in law enforcement control since the August 13, 2019, apprehension.

12. I believe Device #1, Device #2, Device #3, and Device #4 will contain information relevant to the subject investigation based upon the law enforcement's prior surveillance of MEDLAR and FISHER. It appeared the two had to be in constant communication with each other prior to their apprehension. Further, Based upon your Affiant's prior training and experience in narcotics investigations, it is my considered opinion that individuals who engage in the drug trafficking commonly utilize cellular telephones to generate and receive voice messages and text messages by and between associates, colleagues and co-conspirators, and also to track drug shipments arriving through the United States Mail. Also through training and experience it common for drug shipments to be sent to one address, picked by someone who is sent and or paid to retrieve that shipment and bring to a desired location. Those engaging in drug trafficking commonly use cellular telephones to notify/alert co-conspirators of the arrival of a shipment, and to notify/alert them of the desired drop off location.

13. Device #1, Device #2, Device #3, and Device #4 are currently in the lawful possession of the United States Postal Inspection Service. It came into the United States Postal Inspection Service's possession in the following way: seized during a search warrant executed at 1310 Danner Ave, Dayton, OH 45417. In my training and experience, I know that Device #1, Device #2, Device #3, and Device #4 have been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as they were when Device #2, and Device #3 first came into the possession of the USPIS and the Montgomery County Sheriff's Office.

TECHNICAL TERMS

14. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

c. Portable media player: A portable media player (or "MP3 Player" or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When

a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.

f. Tablet: A tablet is a mobile computer, typically larger than a phone yet smaller than a notebook, that is primarily operated by touching the screen. Tablets function as wireless communication devices and can be used to access the Internet through cellular networks, 802.11 "wi-fi" networks, or otherwise. Tablets typically contain programs called apps, which, like programs on a personal computer, perform different functions and save data associated with those functions. Apps can, for example, permit accessing the Web, sending and receiving e-mail, and participating in Internet social networks.

g. Pager: A pager is a handheld wireless electronic device used to contact an individual through an alert, or a numeric or text message sent over a telecommunications network. Some pagers enable the user to send, as well as receive, text messages.

h. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

i. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

15. Based on my training, experience, and research, and from consulting the manufacturer's advertisements and product technical specifications available online at https://www.lg.com/us/cell-phones/lg-M153-fortune;https://www.backmarket.com/tested-and-certified-used-zte-grand-x-max-2-16-gb-blue-cricket/55586.html?gclid=EAIaIQobChMIjK2g19zY5QIVKSCtBh3k-wjwEAQYASABEgLWXfD_BwE;https://www.phonearena.com/phones/ZTE-Sonata-3_id10187; https://www.kyoceramobile.com/duraxt/. I know that the Devices have capabilities that allow it to serve as "a wireless telephone, digital camera, portable media player, GPS navigation device, and PDA." In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

16. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

17. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Device because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

18. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

19. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

20. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Device described in Attachment A to seek the items described in Attachment B.

REQUEST FOR SEALING

21. It is respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the application and search warrant. I believe that sealing this document is necessary because the warrant is relevant to an ongoing investigation into the criminal organizations as not all of the targets of this investigation will be searched at this time. Based upon my training and experience, I have learned that, online criminals actively search for criminal affidavits and search warrants via the internet, and disseminate them to other online criminals as they deem appropriate, i.e., post them publicly online through the carding forums. Premature disclosure of the contents of this affidavit and related documents may have a significant and negative impact on the continuing investigation and may severely jeopardize its effectiveness.

Respectfully submitted,

Joseph Rossiter, Postal Inspector
United States Postal Inspection Service

Subscribed and sworn to before me
On January 3rd, 2020:

Hon. Sharon L. Ovington
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

4. The property to be searched is a black, LG-M153: IMEI: 354064064089453326, S/N: 709CQJZ945332, FCC ID: ZNFM150, hereinafter "Device #1;" a black, ZTE Grand X Max2: SKU: DZTK4120, IMEI: 868962022957502, S/N: 320173713308, hereinafter "Device #2;" a black LG Z832: FCCID: SRQ-Z831, IMEI: 869627024081713, S/N: 328C66800E39, SKU: DZTK4021, hereinafter "Device #3;" and Kyocera E4277: FCC ID: V65E4255, DEC: 268435459912517369, HEX: A0000027BEFFF9, hereinafter "Device #4." The Devices are currently located at the United States Postal Inspection Service Office, 1111 East 5th St, Dayton, OH 45401.

This warrant authorizes the forensic examination of the Device for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

1. All records on the Device described in Attachment A that relate to violations of 21 U.S.C. § 846, 841(a)(1) (conspiracy to possess with the intent to distribute a controlled substance) and involve Johnny MEDLAR, Deshan FISHER and Andre PHILLIPS, including:

   a. lists of customers and related identifying information;

   b. types, amounts, and prices of drugs trafficked as well as dates, places, and amounts of specific transactions;

   c. any information related to sources of drugs (including names, addresses, phone numbers, or any other identifying information);

   d. any information recording MEDLAR'S schedule or travel;

   e. all bank records, checks, credit card bills, account information, and other financial records.

   f. Any and all evidence of user attribution showing who used or owned the device at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;

2. Evidence of user attribution showing who used or owned the Device at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;